Curves of every genus with many points. I: Abelian and toric families

Kresch, A ; Wetherell, J ; Zieve, M E

Abstract: Let Nq(g) denote the maximal number of Fq-rational points on any curve of genus g over Fq. Ihara (for square q) and Serre (for general q) proved that lim supg→∞ Nq(g)/g > 0 for any fixed q. Here we prove limg→∞ Nq(g) = ∞. More precisely, we use abelian covers of 1 to prove lim infg→∞ Nq(g)/(g/log g) > 0, and we use curves on toric surfaces to prove lim infg→∞ Nq(g)/g1/3 > 0; we also show that these results are the best possible that can be proved using these families of curves. © 2002 Elsevier Science (USA).

DOI: https://doi.org/10.1006/jabr.2001.9081

CURVES OF EVERY GENUS WITH MANY POINTS, I: ABELIAN AND TORIC FAMILIES

ANDREW KRESCH, JOSEPH L. WETHERELL, AND MICHAEL E. ZIEVE

ABSTRACT. Let $N_q(g)$ denote the maximal number of $\mathbb{F}_q$-rational points on any curve of genus g over $\mathbb{F}_q$. Ihara (for square q) and Serre (for general q) proved that $\limsup_{g\to\infty} N_q(g)/g > 0$ for any fixed q. Here we prove $\lim_{g\to\infty} N_q(g) = \infty$. More precisely, we use abelian covers of $\mathbb{P}^1$ to prove $\liminf_{g\to\infty} N_q(g)/(g/\log g) > 0$, and we use curves on toric surfaces to prove $\liminf_{g\to\infty} N_q(g)/g^{1/3} > 0$; we also show that these results are the best possible that can be proved using these families of curves.

1. INTRODUCTION

Let $\mathbb{F}_q$ be the field with q elements, and let C be a curve (nonsingular, projective, geometrically irreducible) of genus g defined over $\mathbb{F}_q$. The Riemann hypothesis for curves over finite fields (Weil's theorem) implies that the number of $\mathbb{F}_q$-rational points on C satisfies the inequality $\#C(\mathbb{F}_q) \le q + 1 + 2g\sqrt{q}$. Ihara [21] showed that, when g is large compared to q, this inequality can be improved significantly. In this paper we study such improvements, seeking the best upper bound on $\#C(\mathbb{F}_q)$ which depends only on g and q – we let $N_q(g)$ denote this bound, i.e., $N_q(g)$ is the maximum number of $\mathbb{F}_q$-rational points on any curve over $\mathbb{F}_q$ of genus g.

The Weil bound implies that, for q fixed and g varying, $N_q(g) \le g(2\sqrt{q}) + O_q(1)$. Ihara [21] observed that equality cannot hold when g is much larger than q, since this would imply the existence of curves having a negative number of points over $\mathbb{F}_{q^2}$. This observation was extended by Drinfeld and Vladut [3] to derive the bound $N_q(g) \le g(\sqrt{q}-1)+o_q(g)$, or in other words (for q fixed) $\limsup_{g\to\infty} N_q(g)/g \le \sqrt{q}-1$.

In order to test the sharpness of the Drinfeld-Vladut bound, it is necessary to produce curves with many points. Five essentially different

The authors thank Andrew Granville, David Harbater, Sandy Kutin, Hendrik W. Lenstra, Jr., Jean-Pierre Serre, Chris Skinner, William Stein, Jeff VanderKam, and Hui Zhu for helpful comments and conversations. The authors were supported in part by NSF Mathematical Sciences Postdoctoral Research Fellowships.

approaches have been used. Serre [26, 29] used class field towers to show that, for any q, we have $\limsup_{g\to\infty} N_q(g)/g \geq \gamma_q > 0$; subsequently, other authors have used the same method to derive the same result but with larger constants γ_q (see [24] and the references therein). Ihara [17, 18, 19, 20, 21] used supersingular points on Shimura curves to show that, when q is a square, one can take $\gamma_q = \sqrt{q}-1$ – the largest constant possible, according to the Drinfeld-Vladut result; subsequently, Manin and Vladut [22] used supersingular points on Drinfeld modular curves to derive the same result. (Some special cases of Ihara's construction were rediscovered in [31].) Garcia and Stichtenoth wrote down explicit towers of Artin-Schreier extensions [11, 12] and (jointly with Thomas) Kummer extensions [13] which have many points (interestingly, Elkies has shown that several of the Garcia-Stichtenoth towers are examples of towers of modular [4] or Drinfeld modular [5] curves). Zink [32] showed that certain degenerate Shimura varieties are curves with many points of degree three over the prime field. The fifth and most recent approach is that of Frey, Kani and Völklein [7], who combine rigidity methods from group theory with a careful analysis of certain abelian varieties in order to produce curves over $\mathbb{F}_q$ having unramified covers of arbitrarily large degree in which some $\mathbb{F}_q$-point splits completely.

The above results exhibit sequences of genera g for which $N_q(g)$ is 'large' (relative to g). In the present paper we examine how small $N_q(g)$ can be (relative to g). Our first new result is

Theorem 1.1. *For fixed q, we have $\lim_{g\to\infty} N_q(g) = \infty$.*

The difficulty in proving this result is that we insist on finding curves in *every* large genus. The methods listed above for producing curves with many points do not enable one to do this (for example, modular curves achieve few genera [2]). On the other hand, the simplest families of curves which do attain every large genus – hyperelliptic, trigonal, bielliptic – are all low-degree covers of low-genus curves, so they cannot have many points. For instance, no curve of these three types can have more than 10 points over $\mathbb{F}_2$, and in fact before the present paper it was not known whether $N_2(g) > 10$ for all large g.

We will give three proofs of Theorem 1.1, based on studying three particular family of curves: tame cyclic covers of $\mathbb{P}^1$, arbitrary abelian covers of $\mathbb{P}^1$, and curves embedded in toric surfaces. In each case we prove a lower bound on $N_q(g)$, and in the abelian and toric cases, we show that (up to a universal constant factor) these are the best lower bounds on $N_q(g)$ provable with these families of curves. For each q and g, let $N_q^{\mathrm{ab}}(g)$ denote the maximum number of $\mathbb{F}_q$-rational points on any genus-g curve which is an abelian cover of $\mathbb{P}^1$ over $\mathbb{F}_q$; let $N_q^{\mathrm{tc}}(g)$

and $N_q^{\mathrm{tor}}(g)$ denote the corresponding quantities for tame cyclic covers of $\mathbb{P}^1$ over $\mathbb{F}_q$ and for curves which embed in toric surfaces over $\mathbb{F}_q$, respectively.

Theorem 1.2. *For any fixed q, there exist constants $0 < a_q < b_q$ such that: for every $g > 1$, we have $a_q \cdot g/\log g < N_q^{\mathrm{ab}}(g) < b_q \cdot g/\log g$.*

Theorem 1.3. *For any fixed q, there exist constants $0 < c_q < d_q$ such that: for every $g > 0$, we have $c_q \cdot g^{1/3} < N_q^{\mathrm{tor}}(g) < d_q \cdot g^{1/3}$.*

Theorem 1.4. *For any fixed q, there exist constants $e_q, f_q > 0$ such that: for every $g > f_q$, we have $e_q \cdot g(\log\log g)/(\log g)^3 < N_q^{\mathrm{tc}}(g)$.*

These three theorems are proved in Sections 2, 3, and 4, respectively. The upper bound in Theorem 1.2 is due to Frey, Perret, and Stichtenoth [8]. The other inequalities are new.

Several authors have previously used abelian covers to produce curves with many points. Serre [26, 29] proposed abelian covers of known curves as a convenient source of curves with many points in case g is not much larger than q, the idea being that such covers can be understood via class field theory. Other authors have subsequently taken this approach to produce numerous examples (cf. [14] or [23]). The hard part in our work is finding examples with prescribed genus. The toric approach of Section 3 is new.

Theorems 1.2 and 1.3 imply that any one genus behaves in roughly the same manner as any other, with respect to the maximum number of $\mathbb{F}_q$-rational points on curves of this genus lying in either of two special families of curves. In subsequent work, we have shown a similar assertion for the family of *all* curves:

Theorem 1.5 ([6])**.** *For any fixed q, there exists $h_q > 0$ such that: for every $g > 0$, we have $h_q \cdot g < N_q(g)$.*

Throughout this paper, by a curve over a field k, or simply 'curve', we mean a complete non-singular one-dimensional variety defined over k which is geometrically irreducible. We reserve the symbol p for the characteristic of the field under consideration.

We advise the reader that the sections of this paper are logically independent from each other, and can be read in any order.

2. Abelian covers of $\mathbb{P}^1$

In this section we prove Theorem 1.2 in the following form, where $N_q^{\mathrm{ab}}(g)$ denotes the maximum number of $\mathbb{F}_q$-rational points on any genus-g curve which admits an abelian cover of $\mathbb{P}^1$ over $\mathbb{F}_q$:

Theorem 2.1. *For any fixed q, we have*

$$\inf_{g>1} \frac{N_q^{\mathrm{ab}}(g)}{g/\log g} > 0 \qquad \textit{and} \qquad \sup_{g>1} \frac{N_q^{\mathrm{ab}}(g)}{g/\log g} < \infty.$$

The upper bound is due to Frey, Perret and Stichtenoth [8]. In this section we prove the lower bound. The specific abelian covers we use will be fiber products of elementary abelian covers with a single degree-2 cover.

First consider elementary abelian p-covers of $\mathbb{P}^1/\mathbb{F}_q$ which are only ramified at $x = 0$. (Here p denotes the characteristic of $\mathbb{F}_q$.) For instance, consider the equations

$$y_0^p - y_0 = x^{-i_0}, \quad y_1^p - y_1 = x^{-i_1}, \quad \dots, \quad y_{n-1}^p - y_{n-1} = x^{-i_{n-1}},$$

where $i_0 < i_1 < \cdots < i_{n-1}$ is an increasing sequence of positive integers coprime to p. It can be shown that these equations define a curve of genus

$$\frac{p-1}{2}\Big((i_0 - 1) + (i_1 - 1)p + \cdots + (i_{n-1} - 1)p^{n-1}\Big).$$

For $p = 2$ and any fixed n, these curves achieve every sufficiently large genus; this is the crux of our proof of Theorem 2.1 for even q (which we give at the end of this section). For odd p, however, the genus of such a curve is divisible by $(p-1)/2$ – a problem we will solve by taking a degree-2 cover of our curve. A more serious problem is that the genus is never congruent to $(p+1)/2$ mod p; to attain every congruence class, we allow ramification at two points.

Lemma 2.2. *Let $i_0 < i_1 < \cdots < i_{n-1}$ and $j_0 < j_1 < \cdots < j_{n-1}$ be increasing sequences of positive integers which are coprime to p. Then the equations*

$$\begin{aligned} y_0^p - y_0 &= x^{-i_0}(x-1)^{-j_0} \\ y_1^p - y_1 &= x^{-i_1}(x-1)^{-j_1} \\ &\vdots \\ y_{n-1}^p - y_{n-1} &= x^{-i_{n-1}}(x-1)^{-j_{n-1}} \end{aligned}$$

describe a curve $C/\mathbb{F}_q$ of genus

$$\frac{p-1}{2}\Big((i_0 + j_0) + (i_1 + j_1)p + \cdots + (i_{n-1} + j_{n-1})p^{n-1}\Big).$$

The map $C \to \mathbb{P}^1_x$ is Galois with Galois group $(\mathbb{Z}/p\mathbb{Z})^n$. It is unramified away from $x = 0$ and $x = 1$; furthermore, $x = \infty$ splits completely in the cover $C \to \mathbb{P}^1$.

Proof. We use standard facts about composita of Artin-Schreier extensions, cf. [15] or [10]. Since the right-hand sides of the defining equations are linearly independent over $\mathbb{F}_p$, the field $L := \mathbb{F}_q(x, y_0, \ldots, y_{n-1})$ is a Galois extension of $\mathbb{F}_q(x)$ with Galois group $(\mathbb{Z}/p\mathbb{Z})^n$, and the genus of L is the sum of the genera of all the degree-p subextensions of L. The formula for the genus now follows from the easy fact that if i and j are positive integers coprime to p, and $f(x) \in \mathbb{F}_q[x]$ has degree less than $i + j$ and is coprime to $x(x-1)$, then the curve over $\mathbb{F}_q$ defined by

$$y^p - y = f(x)x^{-i}(x-1)^{-j}$$

has genus $((p-1)/2)(i+j)$. The remaining assertions are clear. □

In our application of this lemma we will want sequences i_ν and j_ν giving a genus on the order of np^n, and moreover we require these sequences to yield such genera in every residue class mod p^n. We address these issues in the following combinatorial lemma.

Lemma 2.3. *Let n and d be positive integers. If p is an odd prime, then there exist increasing sequences $i_0 < \cdots < i_{n-1}$ and $j_0 < \cdots < j_{n-1}$ of positive integers coprime to p such that each $i_k + j_k < (p+3)(k+1)$ (for $0 \le k \le n-1$) and $\sum_{k=0}^{n-1}(i_k + j_k)p^k \equiv d \pmod{p^n}$.*

Proof. We prove the lemma by induction on n. Throughout the proof, if r is an integer, then r_p denotes the unique integer such that $0 \le r_p \le p-1$ and $r_p \equiv r \pmod{p}$. For $n = 1$ we must find positive integers i_0 and j_0 which are coprime to p such that $d \equiv i_0 + j_0 \pmod{p}$ and $i_0 + j_0 < p + 3$. This is easily done: if $d_p > 1$, then set $i_0 = d_p - 1$ and $j_0 = 1$; and if $d_p \le 1$, then set $i_0 = d_p + 1$ and $j_0 = p - 1$.

Now assume, inductively, that we have sequences $i_0 < \cdots < i_{n-2}$ and $j_0 < \cdots < j_{n-2}$ of positive integers coprime to p such that each $i_k + j_k < (p+3)(k+1)$ and $S := \sum_{k=0}^{n-2}(i_k + j_k)p^k$ is congruent to $d \pmod{p^{n-1}}$. We will find integers i_{n-1} and j_{n-1} which are coprime to p, where $i_{n-2} < i_{n-1}$ and $j_{n-2} < j_{n-1}$, such that $i_{n-1} + j_{n-1} < (p+3)n$ and $S + (i_{n-1} + j_{n-1})p^{n-1} \equiv d \pmod{p^n}$. This last congruence is equivalent to $i_{n-1} + j_{n-1} \equiv d' \pmod{p}$, where $d' = (d - S)p^{1-n}$. Now we let

$$i_{n-1} = i_{n-2} + b \quad \text{and} \quad j_{n-1} = j_{n-2} + 1 + (d' - 1 - b - i_{n-2} - j_{n-2})_p,$$

where $b \in \{1, 2, 3\}$ is chosen so that i_{n-1} and j_{n-1} are both coprime to p. Then the desired conditions on i_{n-1} and j_{n-1} are satisfied, and we have completed the induction. □

We now prove Theorem 2.1, first for odd q and then for even q.

Proof of Theorem 2.1 for odd q. Fix a finite field $\mathbb{F}_q$ of characteristic $p > 2$. Let $f(x) \in \mathbb{F}_q[x]$ be a monic irreducible polynomial of even degree. For any $n > 0$, consider the system of equations

$$\begin{aligned} y_0^p - y_0 &= x^{-i_0}(x-1)^{-j_0} \\ y_1^p - y_1 &= x^{-i_1}(x-1)^{-j_1} \\ &\vdots \\ y_{n-1}^p - y_{n-1} &= x^{-i_{n-1}}(x-1)^{-j_{n-1}} \\ y^2 &= f(x), \end{aligned}$$

where both $i_0 < i_1 < \cdots < i_{n-1}$ and $j_0 < j_1 < \cdots < j_{n-1}$ are increasing sequences of positive integers coprime to p. This is the fiber product of a degree-p^n cover $\phi\colon C \to \mathbb{P}^1_x$ (as discussed in Lemma 2.2) with a degree-2 cover ψ from the curve $y^2 = f(x)$ to $\mathbb{P}^1_x$. Since the two covers have coprime degrees, the system of equations describes a curve $\widetilde{C}$ over $\mathbb{F}_q$. Moreover, the induced degree-$2p^n$ cover $\widetilde{C} \to \mathbb{P}^1_x$ is abelian, since it is the fiber product of abelian covers. Write the degree of the different of ψ as $2D$. Then by the Riemann-Hurwitz formula applied to $\widetilde{C} \to C$, the genus $\widetilde{g}$ of $\widetilde{C}$ is given by

$$\widetilde{g} = (p-1)\big((i_0+j_0) + (i_1+j_1)p + \cdots + (i_{n-1}+j_{n-1})p^{n-1}\big) + p^n D - 1.$$

Since f is monic and has even degree, $x = \infty$ splits completely under the map $\widetilde{C} \to \mathbb{P}^1_x$, so $\widetilde{C}$ has at least $2p^n$ rational points over $\mathbb{F}_q$.

Pick any $g > p^2+3p$; we now describe choices of the parameters above so that $\widetilde{g} = g$. Let n be the largest integer such that $(p+3)np^n < g$. Our assumption implies $n \geq 1$. Lemma 2.3 yields sequences $i_0 < i_1 < \cdots < i_{n-1}$ and $j_0 < j_1 < \cdots < j_{n-1}$ of positive integers coprime to p such that each $i_k + j_k < (p+3)(k+1)$ and $\sum_{k=0}^{n-1}(i_k+j_k)p^k$ is congruent to $(g+1)/(p-1)$ mod p^n. Define D by the equation

$$g = (p-1)\sum (i_k + j_k)p^k + p^n D - 1.$$

Then D is an integer, and our bound on $i_k + j_k$ implies D is positive. Let $f(x)$ be a monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree $2D$; then the degree of the different of the degree-2 cover from $y^2 = f(x)$ to $\mathbb{P}^1_x$ is $2D$. Now f, i_k, and j_k satisfy all the conditions of the previous paragraph, and yield a curve $\widetilde{C}$ of genus g such that $\#\widetilde{C}(\mathbb{F}_q) \geq 2p^n$. Our choice of n implies that $\log g > n \log p$ and $p^n \geq g/(p(p+3)(n+1))$, so

$$\#\widetilde{C}(\mathbb{F}_q) \cdot \log g > 2p^n \cdot n \log p \geq \frac{2\log p}{(p+3)p}\frac{n}{(n+1)}g \geq \frac{\log p}{2p^2}g.$$

We have shown that $\inf_{g>p^2+3p} N_q^{\mathrm{ab}}(g)/(g/\log g)$ is positive. To complete the proof, we must show that $N_q^{\mathrm{ab}}(g) > 0$ for all $g > 1$. For this, let $h(x) \in \mathbb{F}_q[x]$ be squarefree of degree $2g+1$, and note that the curve $y^2 = h(x)$ has genus g and has an $\mathbb{F}_q$-rational point. □

Proof of Theorem 2.1 for even q. Let $i_0 < i_1 < \cdots < i_{n-1}$ be an increasing sequence of odd positive integers, and consider the system of equations

$$y_0^2 + y_0 = x^{-i_0}, \quad y_1^2 + y_1 = x^{-i_1}, \quad \ldots, \quad y_{n-1}^2 + y_{n-1} = x^{-i_{n-1}}.$$

Just as in the proof of Lemma 2.2, we see that these equations define a curve C over $\mathbb{F}_2$ such that $\#C(\mathbb{F}_2) \geq 2^n$ and the genus of C is

$$\frac{i_0 - 1}{2}2^0 + \frac{i_1 - 1}{2}2^1 + \cdots + \frac{i_{n-1} - 1}{2}2^{n-1}.$$

For a fixed positive integer n, we can find sequences i_k as above yielding curves of any genus greater than $n2^{n+1} - 5$: there is a unique choice of $i_0 \in \{1, 3\}$, $i_1 \in \{5, 7\}$, $\ldots$, $i_{n-2} \in \{4n-7, 4n-5\}$ for which $\sum_{k=0}^{n-2}(i_k - 1)2^{k-1}$ attains any prescribed integer value in the interval $[(n-3)2^n + 4, (n-3)2^n + 2^{n-1} + 3]$, and for any $g \geq n2^{n+1} - 4$ there is then an odd integer $i_{n-1} > 4n - 5$ yielding a genus-g curve.

For a given nonnegative integer g, let n be the unique positive integer such that $n2^{n+1} - 4 \leq g < (n+1)2^{n+2} - 4$. Then the previous paragraph shows that $N_q^{\mathrm{ab}}(g) \geq 2^n$, and for $g > 1$ this implies that $N_q^{\mathrm{ab}}(g) > ((\log 2)/4) \cdot g/\log g$. □

3. Curves in toric surfaces

Curves in toric surfaces are those given by a single equation $f(x, y) = 0$, such that the curve in $\mathbb{P}^2$ defined by f has a resolution of singularities of a specific form. As we explain below, the genus and number of rational points of such a curve are governed by the shape of the defininining equation $f(x, y)$—specifically, by the Newton polygon of f. Letting $N_q^{\mathrm{tor}}(g)$ denote the maximum number of $\mathbb{F}_q$-rational points on any genus-g curve which embeds in a toric surface over $\mathbb{F}_q$, we will prove Theorem 1.3 in the following form:

Theorem 3.1. *For any fixed q, we have*

$$\inf_{g>0} \frac{N_q^{\mathrm{tor}}(g)}{g^{1/3}} > 0 \qquad \textit{and} \qquad \sup_{g>0} \frac{N_q^{\mathrm{tor}}(g)}{g^{1/3}} < \infty.$$

The following result presents the curves we use to prove the lower bound.

Proposition 3.2. *Let k be a field of characteristic $p > 0$, and let r be a positive integer. Choose integers $0 < a_0 < \cdots < a_r$. Then the equation $f(x, y) = 0$, where*

$$f(x,y) := 1 + y + x^{r+1} + \sum_{i=0}^{r} x^i y^{p(a_i + \cdots + a_r)},$$

defines a curve over k with at least r rational points and genus

$$g := -r + p\sum_{i=0}^{r} i a_i. \tag{1}$$

Moreover, this curve has a smooth complete model in some smooth projective toric surface over k.

Remark. The *Newton polygon* of a polynomial $f \in k[x, y]$ is the convex hull in $\mathbb{R}^2$ of the set of lattice points (i, j) for which the coefficient of $x^i y^j$ in f is nonzero. The expression for the genus (1) is the number of interior lattice points in the Newton polygon of f.

Proposition 3.2 is an immediate consequence of the following algebro-geometric statement.

Proposition 3.3. *Let k be a field. Let $f \in k[x, y]$ satisfy*

(i) *f, $\partial f/\partial x$, and $\partial f/\partial y$ generate the unit ideal in $k[x, y]$;*
(ii) *f has nonzero constant term, and f is not in $k[x]$ or $k[y]$;*
(iii) *every lattice point on the boundary of the Newton polygon of f is either a vertex or lies on the horizontal or vertical coordinate axis.*

Let g be the number of lattice points in the interior of the Newton polygon of f, and let v be the number of vertices of the Newton polygon. Then $f(x, y) = 0$ defines a curve which has genus g and at least $v - 2$ rational points over k. Moreover, the curve admits a smooth complete model in some smooth projective toric surface over k.

The plan for the rest of this section is as follows. Given Proposition 3.3, the lower bound of Theorem 3.1 follows by easy combinatorics, which we do first. The upper bound uses known combinatorics of lattice polygons, coupled with some geometry of curves in algebraic surfaces. This bit of algebraic geometry is also what is needed to prove Proposition 3.3, and we present this second. Lastly, we establish the upper bound in Theorem 3.1.

Proof that Proposition 3.3 implies the lower bound of Theorem 3.1. For any $g > 0$, there is a genus-g curve which has at least one $\mathbb{F}_q$-rational point and which satisfies (i)–(iii) of Proposition 3.3: for instance, let $h(x) \in \mathbb{F}_q[x]$ be squarefree of degree $2g + 1$, and take $y^2 + y = h(x)$

for even q and $y^2 = h(x)$ for odd q. Thus, it suffices to show that for sufficiently large g there exist curves in toric surfaces whose genus is bounded above by a constant times the cube of the number of rational points. Moreover, it suffices to consider the case where q is a prime p.

We use Proposition 3.2 (which follows at once from Proposition 3.3). We may consider each residue class of g mod p separately. By dint of (1), we are reduced to showing that for r in a given residue class mod p, there are increasing nonnegative sequences $\{a_i\}$ with g/r^3 bounded, so that the sums $\sum_{i=0}^{r} ia_i$ take on all sufficiently large positive integers. Consider sequences $\{a_i\}$ with $a_0 = 0, \ldots, a_{r-2} = r-2$ and $r-1 \leq a_{r-1} \leq 2(r-1) < a_r$. Since nonnegative linear combinations of $r-1$ and r achieve all integer values greater than r^2, there are sequences of this type (for fixed r) for which $\sum_{i=0}^{r} ia_i$ takes on any prescribed value greater than $(2r^3 + 15r^2)/6$. This proves the lower bound in Theorem 3.1. □

Now we prove Proposition 3.3. Any $f(x, y)$ satisfying (i)–(iii) defines a variety on a suitable toric surface having the claimed (arithmetic) genus by a result in [16], but it is not immediately clear that this variety is a curve (i.e., smooth and geometrically irreducible). So we need to show more: examination of its defining equations in coordinate charts establishes smoothness, and then a little intersection theory eliminates the possibility of geometric reducibility. Given the analysis we need for this, the genus computation falls out easily; for more general results see [16]. The reader is only assumed to know basic facts about toric varieties, particularly about toric surfaces; cf. [9].

Lemma 3.4. *Let k be a field. Let $f(x, y) \in k[x, y]$ be a nonzero polynomial, and let Γ be the Newton polygon of f. Then the variety defined by $f(x, y) = 0$ can be compactified to a variety V in a smooth projective toric surface Y, such that V is disjoint from the set of fixed points for the toric action on Y. Moreover, for any smooth projective toric surface Y admitting such a compactification V, the arithmetic genus of V is equal to the number of lattice points in the interior of Γ.*

Proof. A toric surface is a two-dimensional normal variety Y, equipped with the action of the two-dimensional algebraic torus $T^2 = (\mathbb{A}^1 \smallsetminus \{0\})^2$ and a dense equivariant embedding $T^2 \to Y$. The combinatorial object attached to Y is a *fan*, which we denote Δ, consisting of cones in a two-dimensional lattice N; the dual lattice $\mathrm{Hom}(N, \mathbb{Z})$ (usually denoted M) is identified with the lattice $\mathbb{Z}^2$ in which the Newton polygon sits (so x and y can be regarded as coordinates on Y). Cones of the fan correspond to affine coordinate charts on Y.

Each ray (one-dimensional cone) of Δ defines a family of half-planes in $\mathbb{Z}^2$, namely $\rho = \mathbb{R}_+ \cdot v$ defines a half-plane $\{\, \alpha \,|\, \alpha(v) \geq h \,\}$ for any $h \in \mathbb{R}$. Let us say that any half-plane in this family is *associated with* ρ. Consider the variety in T^2 defined by the equation $f(x, y) = 0$, with closure V in Y. We show now, by transforming f into local coordinate systems, that a complete toric surface Y has all its fixed points disjoint from V if and only if every supporting half-plane which meets Γ in an edge is associated with some ray $\rho \in \Delta$. Indeed, consider a two-dimensional cone $\nu = \mathbb{R}_+ \cdot v + \mathbb{R}_+ \cdot w$; the corresponding affine chart U_ν has coordinate ring $k[G_\nu]$, where G_ν is the semigroup

$$\{\, \alpha \in \mathrm{Hom}(N, \mathbb{Z}) \,|\, \alpha(v) \geq 0 \text{ and } \alpha(w) \geq 0 \,\}.$$

Now V is disjoint from the origin of U_ν if and only if there is an element in $k[G_\nu]$, with nonzero constant term, which is equal to $f(x, y)x^r y^s$ for some integers r and s. Such an element exists if and only if some translate of Γ is contained in G_ν and contains the origin, i.e., if the corner point of the intersection of the pair of supporting half-planes of Γ associated with v and with w is a vertex of Γ.

The nonsingular toric surfaces are those with $U_\nu \simeq \mathbb{A}^2$ for every two-dimensional cone $\nu \in \Delta$, or equivalently, with every two-dimensional cone generated by vectors which form a $\mathbb{Z}$-basis for N. In this case we say Δ is *nonsingular*. A toric surface is projective if and only if it is a complete variety, and this is the case if and only if the union of the cones in its fan is equal to N: such a fan is called *complete*.

Any finite set of rays in N is contained in a nonsingular complete fan Δ. Consequently, given any nonzero polynomial $f(x, y)$, there exists a nonsingular projective toric surface Y such that the subvariety V of Y defined by $f(x, y) = 0$ (as above) is disjoint from the fixed points of Y. Now we consider the long exact sequence of sheaf cohomology groups

$$H^1(Y, \mathcal{O}_Y) \to H^1(V, \mathcal{O}_V) \to H^2(Y, \mathcal{O}_Y(-V)) \to H^2(Y, \mathcal{O}_Y). \tag{2}$$

The first and last terms in (2) vanish because they are invariant under blowing up a rational point on a projective surface, and they vanish for $\mathbb{P}^2$. So the arithmetic genus of V is equal to $\dim H^2(Y, \mathcal{O}_Y(-V))$. By Serre duality this equals $\dim H^0(Y, K_Y(V))$, where K_Y is the canonical bundle of Y. But $-K_Y$ is the sum of the toric divisors (closures of one-dimensional torus orbits) of Y, so one can identify the set of lattice points in the interior of Γ with a basis for $H^0(Y, K_Y(V))$. □

We continue with the notation of the Lemma – toric surface Y with subvariety V disjoint from the fixed point set of Y – and we describe the intersection of V with any of the one-dimensional torus orbits of Y. Let $\rho = \mathbb{R}_+ \cdot v$ be a ray of Δ, and consider the corresponding torus

orbit E. Corresponding to ρ is a toric chart U_ρ, and we can identify $U_\rho \simeq \operatorname{Spec} k[t, u, u^{-1}]$ so that $t = 0$ defines E. Transforming f into (t, u)-coordinates and setting $t = 0$ yields

$$V \cap E \simeq \operatorname{Spec} k[u, u^{-1}]/(p(u)), \tag{3}$$

where $p(u)$ is the Laurent polynomial whose sequence of coefficients, indexed by $\mathbb{Z}$, is equal to the sequence of coefficients of monomials $x^i y^j$ of f, for (i, j) lying on the boundary ℓ of the half-plane supporting Γ, associated with ρ (the identification of $\mathbb{Z}$ with the set of lattice points on ℓ is to be via an affine linear map, so $p(u)$ is defined only up to multiplication by a power of u and interchanging u and u^{-1}).

If we understand the degree of the Laurent polynomial $p(u)$ to be the maximal degree minus the minimal degree of all the monomials appearing in $p(u)$, then the degree of $p(u)$ is one less than the number of lattice points in $\ell \cap \Gamma$. In particular, if the ℓ associated with ρ contains no lattice points in Γ other than vertices of Γ, then $p(u)$ has degree 0 or 1. Hence the intersection $V \cap E$ is either empty or consists of a single k-valued point, which is a regular point of V.

Now suppose $f(x, y)$ satisfies (i)–(iii) of Proposition 3.3. Since, by (ii), Γ is contained in the first quadrant of $\mathbb{Z}^2$ and contains the origin, there exists a smooth projective toric surface Y with fixed point set disjoint from V, such that Y is obtained by starting with $\mathbb{P}^2$ and repeatedly blowing up points in the complement of $\mathbb{A}^2 \subset \mathbb{P}^2$. Now, then, the test for $V \cap \mathbb{A}^2$ to be nonsingular is precisely condition (i). Additionally, every point of V which is not in $\mathbb{A}^2$ is a regular point of V by condition (iii) and the previous paragraph. Hence V is nonsingular. The genus assertion is Lemma 3.4, and V has at least $v - 2$ rational points, one from each of $v-2$ intersections (3) with $\deg p(u) = 1$ (where v is the number of vertices of the Newton polygon). It remains only to show that V is absolutely irreducible.

We pass to the algebraic closure of k, and we suppose $f = f_1 f_2$ with neither f_1 nor f_2 constant. Equivalently, this means that over the algebraic closure, we can write $V = V_1 \cup V_2$ nontrivially. Since V is nonsingular, this must be a disjoint union. We get a contradiction, and hence a proof of Proposition 3.3, by showing the intersection number $V_1 \cdot V_2$ cannot be zero. By the Riemann-Roch formula for the surface Y, we have $\frac{1}{2} V \cdot V = \operatorname{Area}(\Gamma)$. Letting Γ_i denote the Newton polygon of f_i, for $i = 1, 2$, we obtain $\frac{1}{2} V_1 \cdot V_2 = \frac{1}{2}[\operatorname{Area}(\Gamma) - \operatorname{Area}(\Gamma_1) - \operatorname{Area}(\Gamma_2)] > 0$. This positive quantity is the *mixed volume* of Γ_1 and Γ_2; cf. [9] or [16]. So V is absolutely irreducible, and Proposition 3.3 is proved.

Proof of upper bound in Theorem 3.1. We use the notation of the proof of Lemma 3.4. Fix q, and let C be a curve of genus g which embeds in a toric surface Y over $\mathbb{F}_q$. Without loss of generality, we may assume Y is nonsingular projective, and has fixed point set (for the torus action) disjoint from C. Since every rational point of C is either in the torus T^2 or in one of the nontrivial intersections (3), the number of rational points on C is at most $(q-1)^2 + (q-1)v$, where v is the number of vertices of the Newton polygon of a defining equation $f(x,y)$ for C (in the coordinates of some toric chart). So, it suffices to show that the minimum number $g(v)$ of interior lattice points in a convex lattice v-gon satisfies

$$g(v) \geq N \cdot v^3 \tag{4}$$

whenever $v \geq v_0$, for appropriate positive constants N and v_0.

Arnol'd [1] showed that any convex lattice v-gon has area at least $(1/8192)v^3$. The desired bound (4) follows by combining this, Pick's theorem, and the observation that there is a g-minimal v-gon with no lattice points on the boundary other than vertices ([25, 30]: removing the triangle bounded by two vertices and one interior edge point of a convex lattice v-gon yields a v-gon with as many or fewer interior lattice points and strictly smaller area). □

4. Tame cyclic covers

In this section we use cyclic, tamely ramified covers of $\mathbb{P}^1$ to produce curves with many points in every genus. Let $N_q^{\mathrm{tc}}(g)$ denote the maximal number of $\mathbb{F}_q$-rational points on any curve C over $\mathbb{F}_q$ of genus g which admits a tame cyclic cover $C \to \mathbb{P}^1$ over $\mathbb{F}_q$. We will show

Theorem 4.1. *For any fixed q, we have*

$$\liminf_{g\to\infty} \frac{N_q^{\mathrm{tc}}(g)}{g(\log\log g)/(\log g)^3} > 0.$$

At the end of this section we discuss possible improvements of this result. Our proof of Theorem 4.1 relies on the following lemma:

Lemma 4.2. *Fix q and $n > 1$. Let ℓ_1 be the least prime not dividing q, and let $\ell_2 < \cdots < \ell_n$ be primes which do not divide $q(q-1)\ell_1$. If q is even, we assume further that $\ell_i \equiv 7 \pmod 8$ for some i. Let $L = \prod_{i=1}^n \ell_i$. Then, for any g such that*

$$g > 1 - L + \frac{L}{2}\sum_{i=2}^{n}(\ell_i - 1)^2, \tag{5}$$

there is a curve $C/\mathbb{F}_q$ of genus g and a tame cyclic cover $C \to \mathbb{P}^1$ (over $\mathbb{F}_q$) of degree L in which some $\mathbb{F}_q$-rational point of $\mathbb{P}^1$ splits completely.

One can obtain $\liminf_{g\to\infty} N_q^{\mathrm{tc}}(g)(\log g)^4/(g \log\log g) > 0$ by taking $\ell_2, \dots, \ell_n$ to be the $n-1$ smallest primes which do not divide $q(q-1)\ell_1$. A slight modification to this choice of primes allows us to save a factor of $\log g$ and thereby prove Theorem 4.1.

Proof that Lemma 4.2 implies Theorem 4.1. Fix q, and let ℓ_1 be the least prime not dividing q. For any $g \geq 0$, define x_g to be the least integer such that

$$g - 1 \leq \frac{\ell_1}{2} \cdot \left(\prod_{\substack{\ell \leq x_g \\ \ell \nmid q(q-1)\ell_1 \\ \ell \text{ prime}}} \ell \right) \cdot \left(-2 + \sum_{\substack{\ell \leq x_g \\ \ell \nmid q(q-1)\ell_1 \\ \ell \text{ prime}}} (\ell - 1)^2 \right). \tag{6}$$

Note that the right side might be only slightly larger than the left, or it might be larger by a factor of as much as (slightly more than) x_g. We will modify the set of primes under consideration in order to find an analogous product which is only slightly smaller than $g-1$; we do this by replacing two (suitably chosen) primes p_1 and p_2 by a third prime p_3.

We now define p_1, p_2, and p_3; each definition makes sense for g sufficiently large. Let p_1 be the smallest prime whose removal from the right side of (6) would reverse the inequality; that is, p_1 is the least prime such that $p_1 \nmid q(q-1)\ell_1$ and

$$g - 1 > \frac{\ell_1}{2p_1} \cdot \Big(\prod_{\ell} \ell \Big) \cdot \Big(-2 - (p_1 - 1)^2 + \sum_{\ell} (\ell - 1)^2 \Big).$$

(Here, and in the remainder of this proof, any sum or product indexed by ℓ is understood to be taken over all primes ℓ such that $\ell \leq x_g$ and $\ell \nmid q(q-1)\ell_1$.) Let p_2 be the largest prime such that $p_2 \leq x_g$ and $p_2 \nmid q(q-1)\ell_1 p_1$. Let p_3 be the largest prime such that

$$\begin{aligned} g - 1 > & \frac{\ell_1 p_3}{2p_1p_2} \cdot \Big(\prod_{\ell} \ell \Big) \cdot \\ & \Big(-2 - (p_1 - 1)^2 - (p_2 - 1)^2 + (p_3 - 1)^2 + \sum_{\ell} (\ell - 1)^2 \Big). \end{aligned} \tag{7}$$

We apply Lemma 4.2 to the set of primes

$$\{\ell_1, \dots, \ell_n\} := \{\ell \leq x_g \colon \ell \nmid q(q-1)p_1p_2,\ \ell \text{ prime}\} \cup \{p_3\} \cup \{\ell_1\}.$$

(The hypotheses of Lemma 4.2 are satisfied when g is sufficiently large, since then $p_3 > \max\{q, \ell_1\}$ and also there will be some i for which $\ell_i \equiv 7$

(mod 8).) It follows that $N_q^{\mathrm{tc}}(g) \geq \prod_{i=1}^n \ell_i = (\prod_\ell \ell) \cdot \ell_1 p_3/(p_1 p_2)$. It remains only to determine the asymptotics when $g \to \infty$.

We can rewrite (6) as

$$\log(g-1) \leq \log(\ell_1/2) + \Big(\sum_\ell \log \ell\Big) + \log\Big(-2 + \sum_\ell (\ell-1)^2\Big). \tag{8}$$

The Prime Number Theorem implies that the right hand side of (8) is asymptotic to x_g as $x_g \to \infty$, so $x_g \sim \log g$. Note that $\sum_\ell (\ell-1)^2$ is asymptotic to $x_g^3/(3\log x_g)$; this is much larger than p_1, p_2, and p_3, since $p_1, p_2 \leq x_g$ and (for x_g large) $p_3 < 5q x_g$. Since the left and right sides of (7) are asymptotic to each other as $x_g \to \infty$, it follows that

$$N_q^{\mathrm{tc}}(g) \geq \frac{\ell_1 p_3}{p_1 p_2} \cdot \Big(\prod_\ell \ell\Big) \sim \frac{2g}{x_g^3/(3\log x_g)} \sim \frac{6g(\log\log g)}{(\log g)^3}.$$

This completes the proof. □

Our proof of Lemma 4.2 uses the following existence result:

Lemma 4.3. *Let $P_1, \dots, P_n, \infty$ be distinct places on $\mathbb{P}^1/\mathbb{F}_q$, with degrees $d_1, \dots, d_n, 1$. Let $\ell_1, \dots, \ell_n$ be positive integers such that $q^{d_i} \equiv 1 \pmod{\ell_i(q-1)}$ for each i. There exists a tame abelian cover $\phi\colon C \to \mathbb{P}^1$ (over $\mathbb{F}_q$) of degree $L := \prod_{i=1}^n \ell_i$ such that ∞ splits completely in C and the genus g of C satisfies*

$$2g - 2 = -2L + L\sum_{i=1}^n \frac{\ell_i - 1}{\ell_i} d_i. \tag{9}$$

Moreover, if the ℓ_i are pairwise coprime then ϕ can be chosen to be cyclic.

Proof of Lemma 4.3. Let $\widehat{\phi}\colon \widehat{C} \to \mathbb{P}^1$ be the maximal tamely ramified abelian cover of $\mathbb{P}^1/\mathbb{F}_q$ which is unramified outside $\{P_1, \dots, P_n\}$ and in which ∞ splits completely. By Class Field Theory for $\mathbb{P}^1$, the Galois group $\widehat{G}$ of $\widehat{\phi}$ fits in a short exact sequence

$$1 \longrightarrow \mathbb{F}_q^\times \xrightarrow{\Delta} \prod_{i=1}^n \mathbb{F}_{q^{d_i}}^\times \longrightarrow \widehat{G} \longrightarrow 1,$$

where Δ is the diagonal embedding into the product. Moreover, the inertia group over the place P_i is the image of $\mathbb{F}_{q^{d_i}}^\times$ in $\widehat{G}$.

Since ℓ_i divides $(q^{d_i}-1)/(q-1)$, the group $G := \prod_{i=1}^n \mathbb{Z}/\ell_i\mathbb{Z}$ is a quotient of $\widehat{G}$; let $\phi\colon C \to \mathbb{P}^1$ be the corresponding cover. Then ϕ is a tame abelian cover with Galois group G in which ∞ splits completely and in which all places outside $\{P_1, \dots, P_n\}$ are unramified. Moreover, the inertia group over the place P_i is $\mathbb{Z}/\ell_i\mathbb{Z}$. Hence the genus g of C satisfies (9).

Finally, if the ℓ_i are pairwise coprime then $G \cong \mathbb{Z}/L\mathbb{Z}$ is cyclic. $\square$

Proof of Lemma 4.2. Assume q is odd, so $\ell_1 = 2$. Let $s_1, \ldots, s_n$ be positive integers which will be specified later. Put $r_1 = 2$ and $r_i = \ell_i - 1$ for $i > 1$; set $d_i = r_i s_i$ for all i. Note that $q^{d_i} \equiv 1 \pmod{\ell_i(q-1)}$ for all i.

An easy count shows that, for any $d > 0$, there are at least d finite places on $\mathbb{P}^1$ of degree d; since $d_i \geq i$, it follows that we can choose distinct finite places $P_1, \ldots, P_n$ on $\mathbb{P}^1$ with degrees $d_1, \ldots, d_n$. Lemma 4.3 yields a tame cyclic cover $C \to \mathbb{P}^1$ (over $\mathbb{F}_q$) of degree $L := \prod_{i=1}^n \ell_i$ such that some $\mathbb{F}_q$-rational point of $\mathbb{P}^1$ splits completely in C and the genus $\widetilde{g}$ of C satisfies

$$2\widetilde{g} - 2 = -2L + L\sum_{i=1}^{n} \frac{\ell_i - 1}{\ell_i} d_i.$$

We must show that, for any g satisfying (5), we can choose the s_i so that $\widetilde{g} = g$. Pick any g satisfying (5). Rewrite the expression for $\widetilde{g}$ as

$$\widetilde{g} - 1 + L = \frac{L}{2} s_1 + \sum_{i=2}^{n} \frac{L}{2\ell_i} (\ell_i - 1)^2 s_i. \tag{10}$$

Note that, for $i > 1$, we have $\widetilde{g} - 1 \equiv s_i L/(2\ell_i) \pmod{\ell_i}$. For each $i > 1$, let s_i be the unique integer such that $1 \leq s_i \leq \ell_i$ and $g - 1 \equiv s_i L/(2\ell_i) \pmod{\ell_i}$. Then $g - 1 \equiv \widetilde{g} - 1 \pmod{L/2}$, so (10) implies there is a unique integer s_1 for which $\widetilde{g} = g$. It remains to show $s_1 > 0$; this follows from (5), since

$$g - 1 + L > \frac{L}{2} \sum_{i=2}^{n} (\ell_i - 1)^2 \geq \sum_{i=2}^{n} \frac{L}{2\ell_i} (\ell_i - 1)^2 s_i = \widetilde{g} - 1 + L - \frac{L}{2} s_1.$$

Finally, we indicate how the argument must be modified to handle the case of even q. It suffices to prove the result for $q = 2$. In this case, let i_0 satisfy $1 < i_0 \leq n$ and $\ell_{i_0} \equiv 7 \pmod 8$. Define r_i as above for $i \neq i_0$, and let $r_{i_0} = (\ell_{i_0} - 1)/2$. As above, there is a tame cyclic cover $C \to \mathbb{P}^1$ (over $\mathbb{F}_2$) of degree $L := \prod_{i=1}^n \ell_i$ such that some $\mathbb{F}_2$-rational point splits completely in C and the genus $\widetilde{g}$ of C satisfies (10). It remains to choose the s_i so that $\widetilde{g} = g$. For $i \notin \{1, i_0\}$, choose s_i as above; for $i = i_0$, let s_i satisfy $1 \leq s_i \leq 2\ell_i$ and $g - 1 + L \equiv s_i (L/\ell_i)((\ell_i - 1)/2)^2 \pmod{2\ell_i}$. Then (5) implies there is a unique positive integer s_1 such that $\widetilde{g} = g$, which completes the proof of Lemma 4.2, and thus the proof of Theorem 4.1. $\square$

Remark. Theorem 4.1 implies that $N_q^{\mathrm{tc}}(g) > C_q \cdot g(\log\log g)/(\log g)^3$ for g sufficiently large, where C_q is a positive constant depending only on

q. We do not know whether this result can be improved. In the opposite direction, we now determine the qualitatively best possible *upper* bound on $N_q^{\mathrm{tc}}(g)$. It was shown in [8] that $N_q^{\mathrm{tc}}(g) < D_q \cdot g/\log g$ for $g > 1$, where D_q is a positive constant depending only on q. The following result shows that this upper bound is best possible, by exhibiting infinitely many g (for each q) such that $N_q^{\mathrm{tc}}(g) > g/\log g$.

Proposition 4.4. *For any fixed q, there are infinitely many g for which we have $N_q^{\mathrm{tc}}(g) > (2\log q)g/\log g$.*

Proof. Fix q. For any $e \geq 4$, put $d = (q^e - 1)/(q - 1)$ and let P, ∞ be places of $\mathbb{P}^1$ of degrees e and 1. Let $C \to \mathbb{P}^1$ be the maximal tame abelian cover in which all places besides P are unramified and in which ∞ splits completely. Then $C \to \mathbb{P}^1$ is a cyclic cover of degree d in which P is totally ramified. Moreover, since ∞ splits completely, the cover $C \to \mathbb{P}^1$ is defined over $\mathbb{F}_q$ and $\#C(\mathbb{F}_q) \geq d$. The genus of C is $g = (d-1)(e/2-1)$. Finally,

$$\frac{g}{d} < \frac{e-1}{2} < \frac{\log(d-1)}{2\log q} \leq \frac{\log g}{2\log q},$$

so $d > (2\log q)g/\log g$ and thus the proof is complete. □

References

[1] Arnold, V. I., Statistics of integral convex polygons, *Funktsional. Anal. i Prilozhen.* **14** (1980), 1–3. [*Funct. Anal. Appl.* **14** (1980), 79–81.]

[2] Csirik, J., Wetherell, J. and Zieve, M., On the genera of $X_0(N)$, preprint, 2000, arXiv:math.NT/0006096.

[3] Drinfeld, V. G. and Vladut, S. G., The number of points of an algebraic curve, *Funktsional. Anal. i Prilozhen.* **17** (1983), 68–69. [*Funct. Anal. Appl.* **17** (1983), 53–54.]

[4] Elkies, N., Explicit modular towers, in: *Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing*, (ed. T. Basar and A. Vardy), Univ. of Illinois at Urbana-Champaign, 1998, pp. 23–32.

[5] Elkies, N., Explicit towers of Drinfeld modular curves, in: *Proceedings of the Third European Congress of Mathematics (Barcelona, 2000)*, to appear. arXiv:math.NT/0005140

[6] Elkies, N., Howe, E., Kresch, A., Poonen, B., Wetherell, J. and Zieve, M., Curves of every genus with many points, II: On a question of Serre, preprint, 2000.

[7] Frey, G., Kani, E. and Völklein, H., Curves with infinite K-rational geometric fundamental group, in: *Aspects of Galois Theory (Gainesville, Fla., 1996)*, London Math. Soc. Lect. Note Ser. **256**, Cambridge Univ. Press, Cambridge, 1999, pp. 85–118.

[8] Frey, G., Perret, M. and Stichtenoth, H., On the different of abelian extensions of global fields, in: *Coding Theory and Algebraic Geometry (Luminy, 1991)*, Lect. Notes in Math. **1518**, Springer-Verlag, New York, 1992, pp. 26–32.

[9] Fulton, W., *Introduction to Toric Varieties*, Ann. of Math. Stud., **131**, Princeton Univ. Press, Princeton, 1993.
[10] Garcia, A. and Stichtenoth, H., Elementary abelian p-extensions of algebraic function fields, *Manuscripta Math.* **72** (1991), 67–79.
[11] Garcia, A. and Stichtenoth, H., A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121** (1995), 211–222.
[12] Garcia, A. and Stichtenoth, H., On the asymptotic behavior of some towers of function fields over finite fields, *J. Number Theory* **61** (1996), 248–273.
[13] Garcia, A., Stichtenoth, H. and Thomas, M., On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3** (1997), 257–274.
[14] van der Geer, G. and van der Vlugt, M., Tables of curves with many points, *Math. Comp.* **69** (2000), 797–810. Updates on `http://www.science.uva.nl/~geer/`
[15] van der Geer, G. and van der Vlugt, M., Fiber products of Artin-Schreier curves and generalized Hamming weights of codes, *J. Combin. Theory Ser. A* **70** (1995), 337–348.
[16] Hovanskii, A. G., Newton polyhedra, and the genus of complete intersections, *Funktsional. Anal. i Prilozhen.* **12** (1978), 51–61. [*Funct. Anal. Appl.* **12** (1978), 38–46.]
[17] Y. Ihara, Algebraic curves mod $\mathfrak{p}$ and arithmetic groups, in: *Algebraic Groups and Discontinuous Subgroups (Boulder, Colo., 1965)*, Proc. Sympos. Pure Math. **9**, Amer. Math. Soc., Providence, 1966, pp. 265–271.
[18] Y. Ihara, *On Congruence Monodromy Problems, Vol. 2*, Department of Mathematics, Univ. of Tokyo, 1969.
[19] Y. Ihara, On modular curves over finite fields, in: *Discrete Subgroups of Lie Groups and Applications to Moduli (Internat. Colloq., Bombay, 1973)*, Oxford Univ. Press, Bombay, 1975, pp. 161–202.
[20] Y. Ihara, Congruence relations and Shimūra curves, in: *Automorphic Forms, Representations, and L-functions (Corvallis, Ore., 1977)*, Proc. Sympos. Pure Math. **33**, Part 2, Amer. Math. Soc., Providence, 1979, pp. 291–311.
[21] Ihara, Y., Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo* **28** (1981), 721–724.
[22] Manin, Y. I. and Vladut, S. G., Linear codes and modular curves, *Itogi Nauki i Tekhniki* **25** (1984), 209–257. [*J. Soviet Math.* **30** (1985), 2611–2643.]
[23] Niederreiter, H. and Xing, C. P., Algebraic curves over finite fields with many rational points, in: *Number Theory (Eger, 1996)*, W. de Gruyter, Berlin, (1998), pp. 423–443.
[24] Niederreiter, H. and Xing, C. P., Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound, *Math. Nachr.* **195** (1998), 171–186.
[25] Rabinowitz, S., On the number of lattice points inside a convex lattice n-gon, *Congr. Numer.* **73** (1990), 99–124.
[26] Serre, J.-P., Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris* **296** (1983), 397–402; = Œuvres [128].
[27] Serre, J.-P., Nombres de points des courbes algébriques sur $\mathbb{F}_q$, *Sém. Théor. de Nombres Bordeaux* (1982–1983), exp. 22; = Œuvres [129].

[28] Serre, J.-P., Résumé des cours de 1983–1984, in: *Ann. Collège de France*, 1984, pp. 79–83; = Œuvres [132].
[29] Serre, J.-P., Rational points on curves over finite fields, unpublished lecture notes by F. Gouvêa, Harvard Univ., 1985.
[30] Simpson, R., Convex lattice polygons of minimum area, *Bull. Austral. Math. Soc.* **42** (1990), 353–367.
[31] Tsfasman, M. A., Vladut, S. G. and Zink, Th., Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982), 21–28.
[32] Zink, Th., Degeneration of Shimura surfaces and a problem in coding theory, in: *Fundamentals of Computation Theory (Cottbus, 1985)*, Lect. Notes in Comput. Sci. **199**, Springer-Verlag, New York, 1985, pp. 503–511.

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104–6395
E-mail address: kresch@math.upenn.edu

Mathematical Sciences Research Institute, Berkeley, CA 94720-5070
E-mail address: jlwether@alum.mit.edu

Hill Center, Department of Mathematics, Rutgers University, 110 Frelinghuysen Road, Piscataway NJ 08854
E-mail address: zieve@math.rutgers.edu